UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNIVERSITY SPORTS PUBLICATIONS CO.,

Plaintiff,

-against-

PLAYMAKERS MEDIA CO., et al.,

Defendants.

09 Civ. 8206 (RJH)

MEMORDUM OPINION AND ORDER

Plaintiff University Sports Publications ("USP") brings this action against defendants, a group of former employees and current competitors, for their roles in an alleged scheme to steal confidential customer and sales information from a USP database. The heart of the case arises under state law: the complaint pleads causes of action for misappropriation of trade secrets, unfair competition, breach of fiduciary duty, and tortious interference with contractual relations. The case comes before this Court, however, because USP also alleges that defendants violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, by accessing the database without authorization (or in excess of their authorization), which offense USP claims caused it to expend $10,500 on two audits to investigate potential system damage.

Defendants moved to dismiss the complaint on the ground that, *inter alia*, it did not adequately plead a CFAA claim. The Court converted the motion to one for summary judgment after it became apparent at oral argument that the pivotal issue was factual: whether any defendant had in fact accessed the database or any portion of the

database without USP's permission. Having received supplemental submissions, the Court finds that the evidentiary record raises a genuine issue of material fact as to this issue.

BACKGROUND

USP sells advertising in sports-related publications. To facilitate business, it maintains an extensive database of customer leads and historical sales data. The database gives USP employees a valuable snapshot of the advertising purchasing habits of potential corporate clients by cataloguing such information as the date, location, cost, and size of a corporation's prior purchases and the names of the corporate employees who authorized the purchases. (Pl. 56.1 ¶¶ 50-51.) USP contends that this information, which took hundreds of man hours to compile and is not readily available to the public, constitutes a trade secret. (Compl. ¶ 65; Pl. 56.1 ¶ 51.) The database, which is password-protected, is housed on computer servers maintained by an information technology contractor, Databasaurus LLC. USP employees access the database remotely through specialized software installed on their work computers. (Pl. 56.1 ¶¶ 52-54.)

Shane Pitta worked as an advertising salesperson at USP from 1995 through 2006. (Def. 56.1 ¶ 24.) He used the database frequently during those eleven years and in the process became friendly with a Databasaurus computer administrator named Darnell Gentles, who serviced the database, had full access to it, and had authority to set access levels for USP employees. (*Id*. at ¶¶ 14-16, 25; Pl. 56.1 ¶ 65.)

Pitta left USP in 2006 and joined its competitor Playmakers two years later, where he colluded, according to plaintiff, with Gentles (who remained at Databasaurus) and Playmakers president Terry Columbus to raid USP's client base by pilfering the

confidential information on the database. The primary evidence of this scheme is the testimony of Michael Acciarito, a disillusioned former Playmakers employee who worked under Pitta and Columbus from December 2008 through July 2009. (Acciarito Aff. ¶ 3.) Acciarito testified that he overheard numerous telephone conversations between Pitta and Gentles in which Pitta asked Gentles to provide him with USP sales data, (*Id.* at ¶¶ 17-18), and that Pitta eventually obtained large amounts of the data and distributed it to Acciarito and other Playmakers employees in an effort to boost the company's sales. (*Id*. at ¶¶ 6-10; Pl. 56.1 at 67-68.) No direct evidence reveals how, exactly, Pitta got the data—there are no dispositive emails or other documents. Certain circumstantial evidence suggests Gentles simply sent it to him. Acciarito testified to observing Pitta access the data through a document on his laptop computer, not through a remotely accessed database. (Acciarito Dep. at 315:21 – 318:2.) This testimony does not preclude the possibility that Pitta obtained the data by accessing USP's system directly and then saving the data to his computer, but the testimony does slightly favor the other explanation (that Gentles sent the data to Pitta rather than granting him access to the database). Moreover, though Databasaurus and another technology contractor both audited the database after learning of the alleged data theft, they discovered no signs of entry by an unauthorized user. (Goldfeder Dep. at 167-70; Zeifman Dep. at 93; Pl. 56.1 ¶¶ 94-101.)

USP resists the conclusion that Pitta received the data from Gentles, rather than taking it directly from the database, because it would mean that Pitta did not violate the CFAA by accessing a computer system without authorization. Plaintiff claims there is at least a triable issue of fact as to whether Pitta accessed the database because, first, he

knew Gentles, who had authority to grant him access, and second, Pitta provided Acciarito with a spreadsheet of sales data which, according to the results of a forensic analysis, had been copied directly from the database. (Pl. 56.1 ¶¶ 69-71.) Given these two facts, USP seeks to have a jury decide whether Pitta copied the spreadsheet himself or whether he simply received it from Gentles.

One piece of evidence, Pitta's laptop, might resolve this dispute conclusively, but it appears to have been destroyed. USP sent Playmakers a letter on July 31, 2009, stating its belief that the laptop contained evidence relevant to the looming litigation and requesting that the machine be preserved. (Pl. 56.1 ¶ 78.) Columbus received this letter and, according to her testimony, placed Pitta's laptop in her desk drawer, "under lock and key," before eventually turning it over to Playmakers' counsel. (*Id*. at ¶ 81.) But the laptop defendants eventually produced to USP is apparently not the laptop Pitta used at Playmakers during the relevant time period. In fact, a forensic examination has revealed that the produced laptop was not used at all during most of Pitta's time at Playmakers. (*Id*. at ¶ 87.) According to plaintiff's expert, the machine had been inactive for four months on July 31, 2009—the date Columbus received the preservation letter—when someone turned it on and, over the ensuing week, began downloading programs and documents to populate the machine's hard drive. (*Id*. at ¶ 92.) The laptop Pitta actually used during the time Acciarito says he misappropriated USP's sales data remains unaccounted for.

The complaint states claims for violation of the CFAA against Pitta and Gentles and for conspiracy to violate the CFAA against all four defendants (Pitta, Gentles, Columbus, and Playmakers). These claims form the lone basis for federal jurisdiction.

The complaint also states claims under state law for misappropriation of trade secrets, unfair competition, breach of fiduciary duty, aiding and abetting breach of fiduciary duty, and tortious interference with contractual relations.

LEGAL STANDARD

Summary judgment is proper if the moving party shows that "there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. Proc. 56(c); *see Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). "In deciding whether there is a genuine issue of material fact as to an element essential to a party's case, the court must examine the evidence in the light most favorable to the party opposing the motion, and resolve ambiguities and draw reasonable inferences against the moving party." *Abramson v. Pataki*, 278 F.3d 93, 101 (2d Cir.2002) (internal quotation marks omitted); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

A party opposing summary judgment "may not rely merely on allegations or denials in its own pleading; rather, its response must—by affidavits or as otherwise provided in this rule—set out specific facts showing a genuine issue for trial." Fed. R. Civ. Proc. 56(e). As the Court has noted, "[t]his requirement has particular relevance when a party's responsive documents are long on speculation and short on specific facts." *Medici Classics Productions, LLC v. Medici Group, LLC*, 683 F.Supp.2d 304, 307 (S.D.N.Y.2010); *see Woodman v. WWOR-TV, Inc.*, 411 F.3d 69, 85 (2d Cir.2005) ("The law is well established that conclusory statements, conjecture, or speculation are inadequate to defeat a motion for summary judgment.").

DISCUSSION

I. CFAA Claims

The CFAA prohibits an enumerated list of computer crimes. 18 U.S.C. § 1030(a)(1) – (7). Though primarily a criminal provision aimed at hacking offenses, the statute creates a private cause of action in certain narrowly defined circumstances. *See* 18 U.S.C. § 1030(g); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130-31 (9th Cir. 2009). Like most CFAA claims, the claims USP asserts against defendants require proof that defendants "intentionally accesse[d] a computer without authorization" or "exceed[ed] authorized access" to a computer.[1] This case turns on the phrases "without authorization" and "exceeds authorized access."[2] The statute does not define "without authorization," though courts have construed it to mean "without any permission." *Id*. at 1133. The statute defines "exceeds authorized access" as follows:

> The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.

---

[1] The provisions under which USP states claims read as follows:

(a) Whoever— . . .

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . .
>
> (C) information from any protected computer; . . .
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value,; or
>
> (5)(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage and loss. . . .

shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030 (2009).

[2] The USP customer database stored on the Databasaurus servers is a "computer" for purposes of the statute. § 1030(e)(1) ("the term 'computer' . . . includes any data storage facility or communications facility directly related to or operating in conjunction with a [data processing device].").

18 U.S.C. § 1030(e)(6). USP maintains that both Gentles and Pitta, through their participation in the misappropriation scheme, accessed the database without authorization or in excess of their authorization. The Court considers the evidence of each defendant's conduct in turn.

A. Gentles

USP admits that Gentles, as a computer systems administrator at Databasaurus, had full access to the database. (Compl. ¶ 30 ("Gentles was authorized to use and access USP's computerized database"); Pl. 56.1 ¶ 10, 15 ("Gentles had full access to the USP database").). Plaintiff argues, however, that Gentles nonetheless accessed the database "without authorization," or at least "exceeded [his] authorized access," by using the database for an improper purpose—namely, to provide Pitta with confidential information.

Plaintiff's theory runs afoul of a persuasive line of recent precedent. Building on earlier case law, the Ninth Circuit and two district courts within the Second Circuit recently held that an employee with authority to access his employer's computer system does not violate the CFAA by using his access privileges to misappropriate information. *LVRC Holdings LLC*, 581 F.3d at 1130-31 ("No language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (Kaplan, J.) ("[R]eading the phrases 'access without authorization' and 'exceeds authorized access' to encompass an employee's misuse or misappropriation of information to which the employee freely was given access and which the employee lawfully obtained would depart from the plain

meaning of the statute."); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, No. 08 Civ. 3980(JS), 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009) (Seybert, J.). These cases rest on three primary rationales. First, the CFAA, by its plain language, prohibits improper "access," not misuse or misappropriation. *LVRC Holdings LLC*, 581 F.3d at 1135; *Jet One Group, Inc.*, 2009 WL 2524864 at *5. Second, because the CFAA is principally a criminal statute, the rule of lenity requires courts to interpret it narrowly. Thus, to the extent the statute is ambiguous as to whether it punishes wrongful use of lawfully obtained access, that ambiguity must be resolved in a defendant's favor. *Id*. at *6; *Orbit One*, 692 F. Supp. 2d at 386. And third, the statute's language and legislative history show that Congress intended it to proscribe hacking, not misappropriation of lawfully accessed information. *Jet One Group, Inc.*, 2009 WL 2524864 at *6.

Plaintiff notes that a different line of precedent construes the CFAA more broadly, to encompass use of a computer for an improper purpose, even if the access itself was lawful. *See, e.g., United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Mktg. Tech. Solutions, Inc. v. Medizine LLC*, No. 09 Civ. 8122 (LLM), 2010 WL 2034404, at *7 (S.D.N.Y. May 18, 2010). These cases are unpersuasive for reasons explained at length in *Orbit One*, *Jet One*, and *LVRC*. Put simply, this other line of cases identifies no statutory language that supports interpreting the CFAA to reach mere misuse or misappropriation of information, let alone language strong enough to justify that interpretation where the rule of lenity counsels a narrow reading. *See LVRC Holdings LLC*, 581 F.3d at 1134-35 (rejecting the analysis in *Citrin*). Accordingly, the Court rejects USP's argument that Gentles, who was

authorized to access the database, violated the CFAA by using the database to misappropriate confidential information.

Next, plaintiff argues that even under the narrow interpretation of the statute, Gentles "exceeded his authorized access" by obtaining information he was not entitled to obtain. In his administrative role, USP contends, Gentles acted as a sort of electronic janitor, performing administrative tasks such as "opening and closing publications, setting access levels for other employees, and running date billings." (Pl. 56.1 ¶ 58.) Though he was given full access to the database and all its contents, (*Id*. at ¶ 13), his job duties did not require him to read or analyze the substantive customer information contained therein. (*Id*. at ¶ 57.) In light of these limited duties, the act of obtaining confidential data and sending it to Pitta fell beyond the scope of Gentles's authorized access, according to plaintiff.

Courts applying the narrow interpretation of the statute have construed the definition of "exceeds authorized access" to apply to a person who uses a limited level of initial access authority to obtain other, more highly protected information that he or she is not entitled to access. *See LVRC*, 581 F.3d at 1133 ("[A] person who 'exceeds authorized access' has permission to access the computer, but accesses information on the computer that the person is not entitled to access."); *Orbit One*, 692 F. Supp. 2d at 385 n.67 ("'[A]n "exceeds authorized access" violation occurs where the defendant first has initial "authorization" to access the computer. But, once the computer is permissibly accessed, the use of that access is improper because the defendant accesses information to which he is not entitled.'") (quoting *Diamond Power Intern, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342 (N.D.Ga. 2007)). In other words, the term "exceeds authorized access," like

the term "access without authorization," requires proof that the offender entered some forbidden virtual space, but the broader term applies to authorized users who cross boundaries set by the system owner, whereas the narrower term covers persons with no access rights at all.

Plaintiff's argument turns on the word "obtain" in the definition of "exceeds authorized access." USP admits Gentles was entitled to *access* all information on the database, but contends he was not entitled to *obtain* that information by providing it to Pitta. This is an elusive distinction. USP does not explain how "accessing" information differs from "obtaining" it. Perhaps the theory is that Gentles had authority to view information on the database (i.e., "access"), but not to copy or download it (i.e., "obtain"). Whatever the theory, the caselaw construes the definition of "exceeds authorized access" to require proof that a user violated limitations on his access rights. *See id*. Thus, USP's admission that Gentles had "full access" to the database forecloses any claim based on his conduct.

Even crediting plaintiff's strained distinction, however, the argument that Gentles "exceeded authorized access" by "obtaining" confidential information to which he was not entitled fails because there is no evidence that Gentles's authority to copy, download, or otherwise gather information from the database was limited. Copying or downloading information may not have been within the scope of Gentles's typical duties, but nothing in the record suggests those actions exceeded his actual authority to use the database. To the contrary, Gentles executed confidentiality agreements with both USP and Databasaurus that clearly contemplated that he would acquire confidential information belonging to USP. (Coll Decl. Ex. E at 1 (agreement between USP and Gentles stating

"the Employer . . . has, and will, continue to transfer [sic] to Employee much of the knowledge and knowhow necessary to obtain advertisers for its publications, names of advertising contacts and advertising pricing policies, names of college, university and academy officials who approve contracts with Employer . . .); Ex. D at ¶4 (agreement between Databasaurus and Gentles stating "[t]he Employee recognizes that the Employer will provide the Employee with confidential information, specialized training, access to the Employer's client base and lists, and access to market information.").) Thus, no reasonable finder of fact could conclude that Gentles exceeded his authority to obtain information by viewing data, downloading data, or through any other action he is alleged to have taken on the database itself. *See LVRC*, 581 F.3d at 1135 n.7 (rejecting claim that technology worker exceeded authorized access by emailing confidential data to personal email account). Of course, the confidentiality agreements also prohibited Gentles from disclosing or divulging USP's confidential information. (Pl. 56.1 ¶ 13.) But while Gentles's alleged violation of those provisions of the confidentiality agreements might sustain a breach of contract, breach of fiduciary duty, or theft of trade secrets claim, it does not, for reasons already discussed, support a CFAA claim. *See Jet One*, 2009 WL 2524864 at *5 (finding that employee did not exceed authorized access by "taking [a] client list from [the employer's] computer for the benefit of the defendant."); *Orbit One*, 692 F. Supp. at 377, 384-86 (no CFAA violation where employees downloaded proprietary information for purpose of competing with employer, in breach of employment agreements). Evidence that Gentles beached the agreements by disclosing information shows that he used the database for an improper purpose, but it does not show that he exceeded his authority to access or obtain information from the database. *Id*.

B. Pitta

The issues concerning Pitta are more straightforward. All parties agree that if Pitta accessed the database after he left USP's employ in 2006, he did so "without authorization." The question is whether the evidentiary record would permit a reasonable trier of fact to conclude that Pitta accessed the database after leaving USP.

Two pieces of circumstantial evidence indicate that Pitta accessed the database illegally. First, while employed at Playmakers, Pitta obtained a spreadsheet that appears to have been copied directly from the database. (Pl. 56.1 ¶¶ 67-73.) Second, during the relevant time period, Pitta maintained contact with Gentles, who had access to the database and authority to set access levels for USP employees. (*Id*. at ¶¶ 18, 65.) Of course, as defendants point out, this evidence, while comporting with plaintiff's theory, also comports with a different version of events: that Gentles, rather than granting Pitta direct access to the database, copied the spreadsheet from the database and sent it to Pitta. And perhaps defendants are correct that the record as a whole favors this second version of the story. USP has found no direct evidence that Pitta or any other unauthorized user ever accessed the database, despite performing two thorough audits of the system after learning of the alleged misappropriation. (Goldfeder Dep. at 167-70; Zeifman Dep. at 93.) And Acciarito, the former Playmakers employee and current USP employee and witness, testified that he observed Pitta accessing the spreadsheet through a file stored on his computer, not through a remotely accessed database (though, as already noted, the possibility remains that Pitta accessed the database earlier, before Acciarito observed him using the saved file). (Acciarito Dep. at 316-17.) On this record, the circumstantial evidence on which USP relies—Pitta's possession of the spreadsheet and his contact with

Gentles—might not be enough, standing alone, to create a genuine issue of material fact that Pitta accessed the database directly. *See LVRC*, 581 F.3d at 1137 ("If the factual context makes the non-moving party's claim of a disputed fact implausible, then that party must come forward with more persuasive evidence than otherwise would be necessary to show that there is a genuine issue for trial."); *Gant ex. rel. Gant v. Wallingford Bd. of Educ.*, 195 F.3d 134, 144 (2d Cir. 1999) ("[W]hile we draw all reasonable inferences in favor of the non-moving party on a motion for summary judgment, we do not permit an issue to go to trial on the basis of mere speculation in favor of the party that bears the burden of proof.").

But the evidence of intentional, bad faith spoliation of Pitta's laptop changes the analysis. "A party's intentional destruction of evidence relevant to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction." *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). A party seeking to benefit from such an inference must establish two elements: first, that the evidence was destroyed with a "culpable state of mind;" and second, that the destroyed evidence was "relevant to the party's claim or defense." *Byrnie v. Town of Cromwell Bd. of Educ.*, 243 F.3d 93, 109 (2d Cir. 2001). At the summary judgment stage, an adverse inference will suffice to create a genuine issue of material fact in "borderline" cases, where the inference is supported by "some (not insubstantial) evidence for the plaintiff's cause of action." *Id*. at 107; *Kronisch*, 150 F.3d at 128.

Here, the record easily satisfies the two elements of the *Byrnie* test. Ample evidence suggests that the laptop—the pivotal piece of physical evidence for determining whether or not Pitta accessed the database—was intentionally destroyed. *See supra* at 4.

A jury could therefore permissibly infer that defendants destroyed the laptop because it contained harmful evidence showing, among other things, that Pitta entered the database without permission. *See Byrnie*, 243 F.3d at 109-10. The closer question is whether this inference finds sufficient support in the record to create a triable issue of fact. *See Kronisch*, 150 F.3d at 128. The Court concludes that the circumstantial evidence of Pitta's illegal access, while not overwhelming, is strong enough to survive summary judgment when paired with the adverse inference a jury could permissibly draw from the spoliation. The record establishes quite clearly that Pitta did in fact possess confidential information taken straight from the database and that Gentles had authority to grant Pitta direct access to the database. Though this evidence leaves something to conjecture, defendants have spoiled the most likely source of conclusive proof. On this record, a jury could reasonably infer that the requisite act of unauthorized access took place. *Kronisch*, 150 F.3d at 128-30.

C. "Loss" under the CFAA

Defendants also argue that summary judgment on the CFAA claims is appropriate because the evidence does not show that USP suffered at least $5,000 in losses.

A plaintiff may only bring a civil action under the CFAA if the defendants' wrongful conduct causes one of the enumerated types of "loss or damage" set forth in subsection (c)(4)(A)(i) of the statute. 18 U.S.C. § 1030(g); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004). Here, plaintiff premises its claims on Clause (I) of that subsection, which covers conduct causing "loss to 1 or more persons during any one-year period . . . aggregating at least $5,000 in value."

The statute defines "loss" as follows:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(d)(7). Under this definition, and under the case law interpreting it from within this circuit, the costs of investigating security breaches constitute recoverable "losses," even if it turns out that no actual data damage or interruption of service resulted from the breach. *See Modis, Inc. v. Bardelli*, 531 F. Supp. 2d 314, 320 (D. Conn. 2008) ("[T]he costs of responding to the offense are recoverable regardless of whether there is an interruption in service, and federal courts have sustained actions based on allegations of costs to investigate and take remedial steps in response to a defendant's misappropriation of data."); *Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, at *8 (S.D.N.Y. Sept. 26, 2006) (denying motion to dismiss because "costs involved in investigating the damage to [a] computer system may constitute . . . loss," even where no actual damage was discovered).[3]

The record contains evidence that USP paid for two audits of the database after learning that defendants may have accessed it without permission: (1) a $1500 network security audit by a contractor named Executive Corporate, Inc.; and (2) a $9000 Databasaurus investigation. (Pl. 56.1 ¶¶94 – 101.) The purpose of the first audit was prophylactic—though perhaps prompted by defendants' conduct, the audit sought to identify ways to improve the database's security systems, not to identify and address damage caused by the security breach that had already taken place. (USP ¶ 96.) As such,

[3] Paragraph 54 of the complaint purports to state a claim under section (a)(5)(C) of the CFAA. That subsection, unlike the other subsections under which USP asserts claims, requires that the plaintiff suffer "damage" as a result of the offense. 18 U.S.C. § 1030 (a)(5)(C). Plaintiff concedes that defendants' conduct did not cause the database any "damage," which the statute defines to require "impairment to the integrity or availability of data, a program, a system, or information . . . ." 18 U.S.C. § 1030 (e)(6). Accordingly, the subsection (a)(5)(C) claim is dismissed.

the cost of the Executive Corporate audit probably does not fall within the statutory definition of "loss." *See Tyco Intern. (US) v. Does*, 2003 WL 23374767, at *3 (S.D.N.Y. Aug. 29, 2003) ("While . . . it is true that the CFAA allows recovery for losses beyond mere physical damage to property, the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system in the wake of a spamming attack."). The Databasaurus audit, in contrast, focused at least in part on investigating defendants' alleged crimes; it sought to identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to resecure the network. (Pl. 56.1 ¶ 100.) The cost of such an investigation constitutes "loss" under the statute. *See Kaufman*, 2006 WL 2807177 at *8; *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1063-65 (S.D. Iowa 2009). Thus, because there is evidence that the Databasaurus audit cost $9000—above the $5000 statutory threshold—there is at least a genuine issue of material fact as to whether plaintiff suffered the requisite loss. *Id.*

* * *

Because genuine issues of material fact exist as to whether Pitta accessed the database without authorization, as well as to whether that offense caused USP at least $5,000 in losses, defendants' motion for summary judgment on the CFAA claims is denied.

II. State Law Claims

In their underlying motion to dismiss the Complaint, defendants challenge the sufficiency of the allegations supporting plaintiff's state law claims.[4] Primarily they argue that an earlier trade secrets case brought by USP against Pitta collaterally estops USP's state law claims in this case. In the earlier case, a New York court held that certain customer-related documents that Pitta allegedly misappropriated when he left USP for a different company (where he worked for two years before joining Playmakers) did not contain "trade secrets." *University Sports Publications Co. v. Arena Media Networks, LLC*, No. 109436/06 (N.Y. Sup. Ct. Aug. 17, 2007) (unpublished).

Under New York law, collateral estoppel (issue preclusion) applies only where "(1) the issue in question was actually and necessarily decided in a prior proceeding, and (2) the party against whom the doctrine is asserted had a full and fair opportunity to litigate the issue in the first proceeding." *Webster v. Wells Fargo Bank, N.A.*, 2009 WL 5178654, at *9 (S.D.N.Y. Dec. 23, 2009) (internal quotation marks omitted). "The party asserting issue preclusion bears the burden of showing that the identical issue was previously decided . . . ." *Colon v. Coughlin*, 58 F.3d 865, 869 (2d Cir. 1995).

Here, the first element of the preclusion doctrine is not satisfied. In the prior action, which was decided before the alleged information theft at issue in this case even took place, USP alleged that Pitta and another former USP employee retained certain,

[4] Even if the CFAA claims did warrant dismissal, the Court would exercise supplemental jurisdiction over the state law claims. The values of "judicial economy, convenience, fairness, and comity" support retaining jurisdiction over the state law claims in the unique circumstances of this case, given that fact discovery has already closed and has given rise to a motion for sanctions, currently pending before Magistrate Judge Freeman, based on the alleged spoliation of the laptop. *See Winter v. Northrup*, 334 Fed. Appx. 344, 345-46 (2d Cir. 2009); *Raucci v. Town of Rotterdam*, 902 F.2d 1050, 1055 (2d Cir. 1990). Requiring a state court to adjudicate contentious discovery matters that occurred before this Court would not foster judicial economy. Moreover, the primary issue that the state law claims raise—whether a database of customer information constitutes a "trade secret"—is far from "novel;" established Court of Appeals doctrine addresses the question. *See Leo Silfen, Inc. v. Cream*, 29 N.Y.2d 387, 392 (1972).

purportedly confidential documents when they left USP. As it turned out, the documents contained publicly available customer data—such as customer "location, industry, main telephone number and web address"—none of which, the New York court concluded, was "secret." *Arena Media Networks, LLC*, No. 109436/06, at 12. In contrast, in this case defendants are accused of wrongfully accessing USP's password-protected database, which, unlike the documents retained in the last case, allegedly contained such decidedly non-public information as customer purchase history—including specific prices customers had paid for advertising in the past—as well as the names of individual contacts at client corporations. Thus, the issue of whether the information at issue in this case constitutes "trade secrets" is not identical to the issue litigated in the prior case, because the information is materially different. Therefore, because the issues decided in the two cases are not the same, collateral estoppel does not bar plaintiff's claims. *See Colon*, 58 F.3d at 869-70.

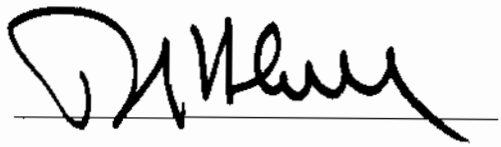
As for the merits of the state law claims, the Court understands from the parties' correspondence that USP has abandoned the tortious interference with contract claim. (Def. May 10, 2010 Ltr. to Magistrate Judge Freeman, at 2.) Accordingly, that claim is dismissed. The Court has considered defendants' arguments concerning the other state law claims and finds them unpersuasive, at least as challenges to the sufficiency of the pleadings; the question of whether the evidentiary record supports those claims is not yet before the Court.

CONCLUSION

For the reasons stated, defendants' converted motion for summary judgment [**58**] is denied. The motion to dismiss [**19**] is granted in part and denied in part.

SO ORDERED.

Dated: New York, New York
July 14, 2010



Richard J. Holwell
United States District Judge